Computer Privacy – What do your surfing habits reveal about you?

As the Internet continues to grow and evolve, more and more people are taking advantage of the benefits it has to offer. From the vast wealth of information available via a standard web browser, to electronic correspondence with friends around the world via e-mail, the Internet has certainly made our lives more productive and enjoyable. However, unknown to most people, the convenience offered by the Internet does have a negative side: The loss of privacy.

What are web bugs

Web Bugs are a very popular means utilized by advertising agencies that assist them in tracking the actions of a user as they browse the web. A web bug is usually a hidden graphic placed within a web page for the purpose of tracking a user. Usually, web bugs are often scaled to a very small size, 1 x 1 pixels, in an effort to hide them from the user. To further conceal them, web bugs are usually set to a transparent background, effectively making them invisible to the user. However, there is no requirement that the image be hidden. Any graphic can be used as a web bug.

How do web bugs work their magic?

Web bugs function on the concept that a web server records information about a user when an image is loaded from a web page. Among the information recorded by the web server that houses the web bug:

- The users IP address.
- The location of the page where the bug is located.
- The location of the web bug itself.
- The time and date the bug was loaded.
- The browser used to retrieve the web bug.
- Any previously set cookies.

It is the last item that is cause for the most concern. Cookies are small files that can be sent to your computer from a web server. Cookies can contain personal information such as you name, address, phone number, etc. that you have supplied to the web site operator. In an effort to protect the information contained within a cookie, a web browser is supposed to send a cookie back to the same server that originally sent the cookie. However, just like any other form of security, there are some technical ways to work around this protection.

Web bugs can be used to gather a variety of statistics about web sites and their users. For example, a web site could place a web bug on the home page so that they can count the number of hits received. All that would have to be done is to analyze the web servers log files for the number of times that particular web bugs was requested. This is the most basic form of a web bug. Advertising companies such as Doubleclick.net can gather and compile this information to form a profile for a given user, tracking the web sites that a user visits.

How do you know if a web bug exists?

There is no easy way to determine if a web page contains a web bug and companies using them are unlikely to advertise their use. You cannot simply filter out all clear image files as they are routinely used to precisely position items within a page. The same holds true for images that are 1 x 1 pixels in size…they too are used for element positioning. To see if a web page contains a web bug, you will need to view the source code of the web page and search for them manually. Viewing the source code of a web page is not difficult. To view the source code using Internet Explorer, select "View" from the menu bar, and then "Source" from the drop down menu.

Searching the source code for a web bug can be a daunting task. Modern websites contain pages that are composed of lengthy and complex elements. To ease the task use the "Find" option of the text editor used for viewing the source code. In notepad, the default text editor for viewing source code within Internet Explorer, select the "Edit" menu item and then "Find" from the drop down list. In the "Find what" dialog box, search for "<IMG" which denotes the start of an image tag. You will need to examine each of the image tags for the signature of a web bug. So what does that signature look like? A web bug typically looks like the following:

```
<IMG WIDTH=1 HEIGHT=1 SRC="http://
media.preferences.com/ping?ML_SD=PGCorporateDM_ProcterAnd
Gamble_1x1_RunOfSite_Any&db_afcr=670A-F384-
15A8E&event=MainPage&group=MainPage&ML_NIF=Y">
```

So what makes this a web bug, or more importantly what do you look for? First, examine the URL from which the image is being retrieved. Does it appear to reside on a server from a well-known information collection company (such as "ad.doubleclick.net")? If it does, chances are you've found a web bug. Perhaps the strongest indicator that you've discovered a web bug is that the image is located on a different server than the one hosting the web page you are viewing. It is rare for a web page to contain elements that are not located on the same server.

The two methods listed above do not conclusively prove the existence of a web bug. The only way to know for certain is to have first hand knowledge of why the web page was designed the way it was. However, they are strong indicators that you have discovered a web bug.

How widely used are web bugs?

Web bugs are widely used on many web sites. I am fortunate enough to have access to my companies firewall logs that record HTTP activity. Reviewing these logs, I discovered that there were 8,943 occurrences of "ad.doubleclick.net" for a single days activity.

Perhaps what is even more telling are the growing number of lawsuits. On January 27, 2000 a lawsuit was brought against DoubleClick. The lawsuit alleges that DoubleClick is violating privacy rights and using deceptive business practices. According to BusinessWeek Online, DoubleClick is considered to be the largest advertising company on the web advertising on more than 1,500 web servers. What is even more staggering is the number of profiles that DoubleClick has built on web surfers: 100 Million. Currently the profiles that have been compiled are anonymous…DoubleClick cannot connect a person to the information. However, in November 1999, DoubleClick purchased Abacus Direct Corp. By doing so, DoubleClick now has the resource it needs in order to link the online profiles to real people.

Another lawsuit filed against Yahoo! Inc. by Universal Image Inc. in the amount of $4 billion demonstrates just how important surfing habits are to companies.

Who uses web bugs?

While researching this topic, I discovered that many well-known companies web sites were using them in one form or another. The following list is an example of the types of businesses utilizing web bugs:

- Proctor and Gamble
- Tide
- Pert Plus
- Bounty
- Pampers

Are there any variations of web bugs?

Yes. Web bugs are not only limited to web surfing with a web browser. Microsoft has gone to great lengths to integrate web services within their latest operating systems and applications. As a result of this integration, web bugs are possible within application programs.

One such example is the presence of web bugs within e-mail messages. Popular e-mail clients, such as Outlook, Outlook Express and Netscape all contain the capability to render e-mail messages that contain web content. Because of this capability these programs will retrieve a web bug from the hosting server in the same manner as a web bug located on a web page. The hosting web server will record the same information about the user as if they were using a web browser. There is one significant difference between web bugs delivered via a web browser and web bugs delivered via an e-mail message: the sender of the web bug already knows the users e-mail address.

How can you protect yourself from web bugs?

Currently, there is little one can do to protect themselves from web bugs. As they are difficult to distinguish from spacer images that normally appear within web pages, they cannot be reliably filtered.

This does not mean that you cannot take steps to minimize the impact of web bugs.

- Cookies can be one of the most revealing aspects of web bugs. You can configure your web browser to reject all cookies, or provide you the opportunity to accept cookies. Thus, when a web bug is encountered, there will not be a cookie that can be passed along. If you decide to turn off cookies, be sure to delete the current ones from your system, as the browser will send any that it already has accepted.

- Use one of many utilities that are designed to manage cookies for your web browser. While they cannot prevent web bugs from being downloaded to your system they can prevent cookies, which may contain private information, from being sent to the interested party. Microsoft's Internet Explorer version 5.5 contains a built in cookie management feature which helps the user to better manage cookies without the need for third party software.

- Be wary of providing information about yourself to companies. Often time's people are asked to provide information about themselves for various reasons. Step back and ask yourself if the information being requested is really necessary.

- If you are really paranoid, you can configure your web browser to avoid downloading image files completely. While this ensures that you do not download web bugs, it effectively removes the benefit of using a web browser.

Are there any positive uses for web bugs?

This is a very subjective question and depends on how strongly you feel about computer privacy. I will not attempt to answer the validity of web bugs in this document. Instead I will suggest a couple of potentially beneficial and non-intrusive uses for web bugs.

I have already given an example where a web bug can be used to count the number of hits to a web page. Another possibility is to utilize the e-mail variant of the web bug to confirm receipt of an e-mail message.

You may be asking how the aforementioned possibilities differ from the intrusive uses of web bugs…after all; the information is still being collected. The answer is quite simple. What makes a web bug a "good" web bug as opposed to a "bad" web bug is how the company collecting the information handles the collected information. Using the web bug counter as an example if the company collecting the hit count information uses it solely for statistics gathering and discards the remaining information, no privacy has been lost.

References:

Bradley, Helen. "Beware Of Web Bugs & Clear GIFs", Smart Computing, Vol. 8 Issue 4. April 2000
http://www.smartcomputing.com/editorial/article.asp?article=articles%2Farchive%2Fg0804%2F11g04%2F11g04%2Easp&guid=rm4behg0&searchtype=0&WordList=web+bugs

Smith, Richard. "The Web Bug FAQ", Version 1.0. November 11, 1999
http://www.tiac.net/users/smiths/privacy/wbfaq.htm

Smith, Richard. "Web Bugs at Proctor and Gamble Web Sites"
http://www.tiac.net/users/smiths/privacy/wbpg.htm

"WEB BUGS, SMALL GRAPHIC OBJECTS THAT CREATE A HIGHWAY FOR INTERNET PRIVACY INVASION", Arawak Net
http://www.arawak.net/pages/web.bugs1.html

Green, Heather. "Privacy: Outrage on the Web", BusinessWeek Online, February 8, 2000
http://businessweek.lycos.com/0002/ls_mk3668065.htm

Josh McKee